

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2002-57997
(P2002-57997A)

(43)公開日 平成14年2月22日(2002.2.22)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
H 0 4 N 7/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
7/081			3 2 0 E 5 C 0 5 2
G 0 6 F 12/14	3 2 0	G 0 9 C 5/00	5 C 0 5 3
		H 0 4 N 5/85	Z 5 C 0 6 3
G 0 9 C 5/00		7/08	Z 5 J 1 0 4

審査請求 未請求 請求項の数142 O L (全 25 頁) 最終頁に続く

(21)出願番号 特願2000-214157(P2000-214157)
(22)出願日 平成12年7月14日(2000.7.14)
(31)優先権主張番号 特願2000-164450(P2000-164450)
(32)優先日 平成12年6月1日(2000.6.1)
(33)優先権主張国 日本(J P)

(71)出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
(72)発明者 佐古 曜一郎
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(74)代理人 100082762
弁理士 杉浦 正知

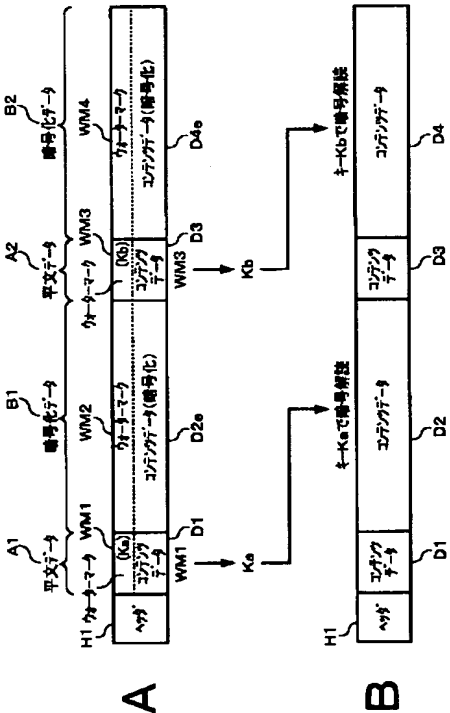
最終頁に続く

(54)【発明の名称】 コンテンツデータ、データ記録媒体、データ記録方法及び装置、データ再生方法及び装置、データ送信方法及び装置、データ受信方法及び装置

(57)【要約】

【課題】 コピー禁止や再生禁止等の著作権の保護に関する情報がウォータマークとして記録されている場合に、再生時に、このウォータマークの情報が確実にデコードされるようにして、著作権の保護が図れるようにする。また、ユーザに見せたい所を確実に見せることができるようにする。

【解決手段】 コンテンツのファイルには、コンテンツのデータを暗号化せずに記録する平文データ部と、コンテンツのデータを暗号化して記録する暗号化データ部とが設けられ、平文データ部では、コンテンツのデータが暗号化せずに記録され、暗号化データ部ではコンテンツのデータが暗号化されて記録される。暗号化のための鍵の少なくとも一部が平文データ部におけるコンテンツのデータに付加情報として埋め込まれる。再生時には、平文データ部のコンテンツのデータに重畳されて記録されているウォータマークに含まれるキー情報を使用して、それに続く暗号化部のデータの復号化処理が行われる。



1

【特許請求の範囲】

【請求項 1】 コンテンツのデータを暗号化せずに配置する平文データ部と、上記コンテンツのデータを暗号化して配置する暗号化データ部とを設け、
上記平文データ部では上記コンテンツのデータを暗号化せずに配置し、上記暗号化データ部では上記コンテンツのデータを暗号化して配置すると共に、
上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたコンテンツデータ。

【請求項 2】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに配置する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して配置する暗号化データ部とを設け、
上記平文データ部では上記コンテンツのデータを少なくとも第 1 の情報では暗号化せずに配置し、上記暗号化データ部では上記コンテンツのデータを上記第 1 の情報と第 2 の情報とを関連させて暗号化して配置すると共に、
上記暗号化されたデータを復号するための上記第 1 の情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたコンテンツデータ。

【請求項 3】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに配置する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して配置する暗号化データ部とを設け、
上記平文データ部では上記コンテンツのデータを第 2 の情報で暗号化して配置し、上記暗号化データ部では上記コンテンツのデータを少なくとも上記第 1 の情報及び／
又は第 2 の情報で暗号化して配置すると共に、
上記第 1 の情報で暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたコンテンツデータ。

【請求項 4】 上記コンテンツのデータは音楽データである請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 5】 上記コンテンツのデータは映像データである請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 6】 上記コンテンツのデータは画像データである請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 7】 上記コンテンツのデータはゲームのデータである請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 8】 上記平文データ部は、上記暗号化データ部に先行して設けるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

2

【請求項 9】 上記平文データ部は、上記コンテンツのデータ部の先頭に設けるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 10】 上記付加情報は、スペクトラム拡散されて、上記コンテンツのデータ中に重畳されるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 11】 上記付加情報は、上記コンテンツのデータの低位ビットに挿入されるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 12】 上記付加情報は、上記コンテンツのデータを圧縮したときの高次係数に挿入されるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 13】 上記付加情報は、マスキング効果を利用して上記コンテンツに影響を与えないように挿入されるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 14】 上記付加情報は、所定範囲の第 1 のピーク若しくは上記第 2 のピーク、又はその近傍に挿入されるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 15】 上記付加情報には、コピー管理情報及び／又は再生管理情報を含めるようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 16】 上記平文データ部には、ユーザに必ず知らせておきたい情報を配置するようにした請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 17】 上記ユーザに必ず知らせておきたい情報は、著作権者についての情報である請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 18】 上記ユーザに必ず知らせておきたい情報は、コンテンツの紹介する情報である請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 19】 上記ユーザに必ず知らせておきたい情報は、注意や警告を示す情報である請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 20】 上記ユーザに必ず知らせておきたい情報は、コマーシャル情報である請求項 1、請求項 2 又は請求項 3 に記載のコンテンツデータ。

【請求項 21】 コンテンツのデータを暗号化して配置する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、
上記平文データ部には上記コンテンツのデータを暗号化せずに配置し、

上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたコンテンツデータ。

【請求項 22】 上記無情報データ部には、無音に相当するオーディオデータを配置するようにした請求項 21

3

に記載のコンテンツデータ。

【請求項 2 3】 上記無情報データ部には、固定パターンに相当するビデオデータを配置するようにした請求項 2 1 に記載のコンテンツデータ。

【請求項 2 4】 上記無情報データ部には、ランダムパターンに相当するビデオデータを配置するようにした請求項 2 1 に記載のコンテンツデータ。

【請求項 2 5】 コンテンツのデータを暗号化せずに記録する平文データ部と、上記コンテンツのデータを暗号化して記録する暗号化データ部とを設け、上記平文データ部では上記コンテンツのデータを暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを暗号化して記録すると共に、上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体。

【請求項 2 6】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、上記平文データ部では上記コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを上記第 1 の情報と第 2 の情報とを関連させて暗号化して記録すると共に、上記暗号化されたデータを復号するための上記第 1 の情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体。

【請求項 2 7】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、上記平文データ部では上記コンテンツのデータを第 2 の情報で暗号化して記録し、上記暗号化データ部では上記コンテンツのデータを少なくとも上記第 1 の情報及び／又は第 2 の情報で暗号化して記録すると共に、上記第 1 の情報で暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体。

【請求項 2 8】 少なくとも第 1 領域及び第 2 の領域の 2 つの領域に分割されており、上記平文データ部を上記第 1 の領域に設け、上記暗号化データ部を上記第 2 の領域に設けるようにした請求項 2 5、請求項 2 6、又は請求項 2 7 に記載のデータ記録媒体。

【請求項 2 9】 上記第 1 の領域と上記第 2 の領域とは記録媒体の外周部と内周部とに分割されている請求項 2 8 に記載のデータ記録媒体。

4

【請求項 3 0】 上記コンテンツのデータは音楽データである請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 3 1】 上記コンテンツのデータは映像データである請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 3 2】 上記コンテンツのデータは画像データである請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

10 【請求項 3 3】 上記コンテンツのデータはゲームのデータである請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 3 4】 上記平文データ部は、上記暗号化データ部に先行して設けるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 3 5】 上記平文データ部は、上記コンテンツのデータ部の先頭に設けるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

20 【請求項 3 6】 上記付加情報は、スペクトラム拡散されて、上記コンテンツのデータ中に重畳されるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 3 7】 上記付加情報は、上記コンテンツのデータの低位ビットに挿入されるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 3 8】 上記付加情報は、上記コンテンツのデータを圧縮したときの高次係数に挿入されるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

30 【請求項 3 9】 上記付加情報は、マスキング効果を利用して上記コンテンツに影響を与えないように挿入されるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 4 0】 上記付加情報は、所定範囲の第 1 のピーク若しくは上記第 2 のピーク、又はその近傍に挿入されるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

40 【請求項 4 1】 上記付加情報には、コピー管理情報及び／又は再生管理情報を含めるようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 4 2】 上記第 2 の情報で暗号化したデータを復号するための情報は、サブコードの領域に記録されている請求項 2 5 又は請求項 2 6 に記載のデータ記録媒体。

【請求項 4 3】 上記第 2 の情報で暗号化したデータを復号するための情報は、リードインに記録されている請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

50 【請求項 4 4】 上記第 2 の情報で暗号化したデータを復号するための情報は、TOC (Table Of Contents) に記録されている請求項 2 6 又は請求項 2 7 に記載のデ

ータ記録媒体。

【請求項 4 5】 上記第 2 の情報で暗号化したデータを復号するための情報は、トラック又はピットのウォブルデータとして記録されている請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 4 6】 上記平文データ部には、ユーザに必ず知らせておきたい情報を記録するようにした請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 4 7】 上記ユーザに必ず知らせておきたい情報は、著作権者についての情報である請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 4 8】 上記ユーザに必ず知らせておきたい情報は、コンテンツの紹介する情報である請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 4 9】 上記ユーザに必ず知らせておきたい情報は、注意や警告を示す情報である請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 5 0】 上記ユーザに必ず知らせておきたい情報は、コマーシャル情報である請求項 2 5、請求項 2 6 又は請求項 2 7 に記載のデータ記録媒体。

【請求項 5 1】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録媒体。

【請求項 5 2】 上記無情報データ部には、無音に相当するオーディオデータを記録するようにした請求項 5 1 に記載のデータ記録媒体。

【請求項 5 3】 上記無情報データ部には、固定パターンに相当するビデオデータを記録するようにした請求項 5 1 に記載のデータ記録媒体。

【請求項 5 4】 上記無情報データ部には、ランダムパターンに相当するビデオデータを記録するようにした請求項 5 1 に記載のデータ記録媒体。

【請求項 5 5】 コンテンツのデータを暗号化せずに記録する平文データ部と、上記コンテンツのデータを暗号化して記録する暗号化データ部とを設け、上記平文データ部では上記コンテンツのデータを暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを暗号化して記録すると共に、上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録方法。

【請求項 5 6】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、

上記平文データ部では上記コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを上記第 1 の情報と第 2 の情報とを関連させて暗号化して記録すると共に、上記暗号化されたデータを復号するための上記第 1 の情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録方法。

【請求項 5 7】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、上記平文データ部では上記コンテンツのデータを第 2 の情報で暗号化して記録し、上記暗号化データ部では上記コンテンツのデータを少なくとも上記第 1 の情報及び／又は第 2 の情報で暗号化して記録すると共に、上記第 1 の情報で暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録方法。

【請求項 5 8】 上記コンテンツのデータは音楽データである請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 5 9】 上記コンテンツのデータは映像データである請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 0】 上記コンテンツのデータは画像データである請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 1】 上記コンテンツのデータはゲームのデータである請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 2】 上記平文データ部は、上記暗号化データ部に先行して設けるようにした請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 3】 上記平文データ部は、上記コンテンツのデータ部の先頭に設けるようにした請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 4】 上記付加情報は、スペクトラム拡散されて、上記コンテンツのデータ中に重畳されるようにした請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 5】 上記付加情報は、上記コンテンツのデータの低位ビットに挿入されるようにした請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 6】 上記付加情報は、上記コンテンツのデータを圧縮したときの高次係数に挿入されるようにした請求項 5 5、請求項 5 6 又は請求項 5 7 に記載のデータ記録方法。

【請求項 6 7】 上記付加情報は、マスキング効果を利

7

用して上記コンテンツに影響を与えないように挿入されるようにした請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 68】 上記付加情報は、所定範囲の第 1 のピーク若しくは上記第 2 のピーク、又はその近傍に挿入されるようにした請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 69】 上記付加情報には、コピー管理情報及び／又は再生管理情報を含めるようにした請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 70】 上記第 2 の情報で暗号化したデータを復号するための情報は、サブコードの領域に記載されている請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 71】 上記第 2 の情報で暗号化したデータを復号するための情報は、リードインに記載されている請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 72】 上記第 2 の情報で暗号化したデータを復号するための情報は、TOC (Table Of Contents) に記録されている請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 73】 上記第 2 の情報で暗号化したデータを復号するための情報は、トラック又はピットのウォブルデータとして記録されている請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 74】 上記平文データ部には、ユーザに必ず知らせておきたい情報を記録するようにした請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 75】 上記ユーザに必ず知らせておきたい情報は、著作権者についての情報である請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 76】 上記ユーザに必ず知らせておきたい情報は、コンテンツの紹介する情報である請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 77】 上記ユーザに必ず知らせておきたい情報は、注意や警告を示す情報である請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 78】 上記ユーザに必ず知らせておきたい情報は、コマーシャル情報である請求項 55、請求項 56 又は請求項 57 に記載のデータ記録方法。

【請求項 79】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録方法。

【請求項 80】 上記無情報データ部には、無音に相当するオーディオデータを記録するようにした請求項 79 に記載のデータ記録方法。

8

【請求項 81】 上記無情報データ部には、固定パターンに相当するビデオデータを記録するようにした請求項 79 に記載のデータ記録方法。

【請求項 82】 上記無情報データ部には、ランダムパターンに相当するビデオデータを配置するようにした請求項 79 に記載のデータ記録方法。

【請求項 83】 コンテンツのデータを暗号化せずに記録する平文データ部と、上記コンテンツのデータを暗号化して記録する暗号化データ部とを設け、

10 上記平文データ部では上記コンテンツのデータを暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを暗号化して記録する手段と、上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込む手段とを備えるようにしたデータ記録装置。

【請求項 84】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、
20 上記平文データ部では上記コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを上記第 1 の情報と第 2 の情報とを関連させて暗号化して記録する手段と、上記暗号化されたデータを復号するための上記第 1 の情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込む手段とを備えるようにしたデータ記録装置。

【請求項 85】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、
30 上記平文データ部では上記コンテンツのデータを第 2 の情報で暗号化して記録し、上記暗号化データ部では上記コンテンツのデータを少なくとも上記第 1 の情報及び／又は第 2 の情報で暗号化して記録する手段と、上記第 1 の情報で暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込む手段とを備えるようにしたデータ記録装置。

【請求項 86】 上記コンテンツのデータは音楽データである請求項 83、請求項 84 又は請求項 85 に記載のデータ記録装置。

【請求項 87】 上記コンテンツのデータは映像データである請求項 83、請求項 84 又は請求項 85 に記載のデータ記録装置。

【請求項 88】 上記コンテンツのデータは画像データである請求項 83、請求項 84 又は請求項 85 に記載のデータ記録装置。

50 【請求項 89】 上記コンテンツのデータはゲームのデ

ータである請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 0】 上記平文データ部は、上記暗号化データ部に先行して設けるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 1】 上記平文データ部は、上記コンテンツのデータ部の先頭に設けるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 2】 上記付加情報は、スペクトラム拡散されて、上記コンテンツのデータ中に重畳されるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 3】 上記付加情報は、上記コンテンツのデータの下位ビットに挿入されるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 4】 上記付加情報は、上記コンテンツのデータを圧縮したときの高次係数に挿入されるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 5】 上記付加情報は、マスキング効果を利用して上記コンテンツに影響を与えないように挿入されるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 6】 上記付加情報は、所定範囲の第 1 のピーク若しくは上記第 2 のピーク、又はその近傍に挿入されるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 7】 上記付加情報には、コピー管理情報及び／又は再生管理情報を含めるようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 8】 上記第 2 の情報で暗号化したデータを復号するための情報は、サブコードの領域に記録されている請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 9 9】 上記第 2 の情報で暗号化したデータを復号するための情報は、リードインに記録されている請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 0】 上記第 2 の情報で暗号化したデータを復号するための情報は、TOC (Table Of Contents) に記録されている請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 1】 上記第 2 の情報で暗号化したデータを復号するための情報は、トラック又はビットのウォブルデータとして記録されている請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 2】 上記平文データ部には、ユーザに必ず知らせておきたい情報を記録するようにした請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 3】 上記ユーザに必ず知らせておきたい

情報は、著作権者についての情報である請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 4】 上記ユーザに必ず知らせておきたい情報は、コンテンツの紹介する情報である請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 5】 上記ユーザに必ず知らせておきたい情報は、注意や警告を示す情報である請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 6】 上記ユーザに必ず知らせておきたい情報は、コマーシャル情報である請求項 8 3、請求項 8 4 又は請求項 8 5 に記載のデータ記録装置。

【請求項 1 0 7】 コンテンツのデータを暗号化して配置する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、

上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録装置。

【請求項 1 0 8】 上記無情報データ部には、無音に相当するオーディオデータを配置するようにした請求項 1 0 7 に記載のデータ記録装置。

【請求項 1 0 9】 上記無情報データ部には、固定パターンに相当するビデオデータを配置するようにした請求項 1 0 7 に記載のデータ記録装置。

【請求項 1 1 0】 上記無情報データ部には、ランダムパターンに相当するビデオデータを配置するようにした請求項 1 0 7 に記載のデータ記録装置。

【請求項 1 1 1】 コンテンツのデータを暗号化せずに記録する平文データ部と、上記コンテンツのデータを暗号化して記録する暗号化データ部とを設け、

上記平文データ部では上記コンテンツのデータを暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを暗号化して記録すると共に、

上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生方法であって、

上記付加情報から暗号化したデータを復号するための情報の少なくとも一部を抜き出し、

上記暗号化したデータを復号するための情報を使って、上記コンテンツのデータを復号化するようにしたデータ再生方法。

【請求項 1 1 2】 コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、

上記平文データ部では上記コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを上記第 1 の情報と第 2 の情報とを関連させて暗号化して記録すると共に、

上記暗号化されたデータを復号するための上記第 1 の情

報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生方法であって、上記付加情報から暗号化したデータを復号するための第1の情報の少なくとも一部を抜き出し、上記暗号化したデータを復号するための第1の情報及び／又は上記第2の情報を使って、上記コンテンツのデータを復号化するようにしたデータ再生方法。

【請求項113】 コンテンツのデータを少なくとも第1の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第1の情報の一部を使って暗号化して記録する暗号化データ部とを設け、上記平文データ部では上記コンテンツのデータを第2の情報で暗号化して記録し、上記暗号化データ部では上記コンテンツのデータを少なくとも上記第1の情報及び／又は第2の情報で暗号化して記録すると共に、上記第1の情報で暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生方法であって、上記平文データ部のデータを第2の情報を使って復号化し、

上記付加情報から暗号化したデータを復号するための第1の情報の少なくとも一部を抜き出し、上記暗号化したデータを復号するための第1の情報及び／又は上記第2の情報を使って、上記コンテンツのデータを復号化するようにしたデータ再生方法。

【請求項114】 上記付加情報には、コピー管理情報及び／又は再生管理情報を含めるようにし、上記コピー管理情報及び／又は再生管理情報を使って、コピーや再生の管理を行うようにした請求項111、請求項112又は請求項113に記載のデータ再生方法。

【請求項115】 上記第2の情報で暗号化したデータを復号するための情報は、サブコードの領域から得るようにした請求項112又は請求項113に記載のデータ再生方法。

【請求項116】 上記第2の情報で暗号化したデータを復号するための情報は、リードインのデータから得るようにした請求項112又は請求項113に記載のデータ再生方法。

【請求項117】 上記第2の情報で暗号化したデータを復号するための情報は、TOC (Table Of Contents) のデータから得るようにした請求項112又は請求項113に記載のデータ再生方法。

【請求項118】 上記第2の情報で暗号化したデータを復号するための情報は、トラック又はピットのウォブルデータから得るようにした請求項112又は請求項113に記載のデータ再生方法。

【請求項119】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行す

る無情報データ部とを設け、

上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生方法であって、

上記付加情報から暗号化したデータを復号するための情報の少なくとも一部を抜き出し、

上記暗号化したデータを復号するための情報を使って、上記コンテンツのデータを復号化するようにしたデータ再生方法。

【請求項120】 上記無情報データ部には、無音に相当するオーディオデータを記録するようにした請求項119に記載のデータ再生方法。

【請求項121】 上記無情報データ部には、固定パターンに相当するビデオデータを記録するようにした請求項119に記載のデータ再生方法。

【請求項122】 上記無情報データ部には、ランダムパターンに相当するビデオデータを配置するようにした請求項119に記載のデータ再生方法。

【請求項123】 コンテンツのデータを暗号化せずに記録する平文データ部と、上記コンテンツのデータを暗号化して記録する暗号化データ部とを設け、

上記平文データ部では上記コンテンツのデータを暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを暗号化して記録すると共に、

上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込む

ようにしたデータ記録媒体を再生するデータ再生装置であって、

上記付加情報から暗号化したデータを復号するための情報の少なくとも一部を抜き出す手段と、

上記暗号化したデータを復号するための情報を使って、上記コンテンツのデータを復号化する手段とを備えるようにしたデータ再生装置。

【請求項124】 コンテンツのデータを少なくとも第1の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第1の情報の一部を使って暗号化して記録する暗号化データ部とを設け、

上記平文データ部では上記コンテンツのデータを少なくとも第1の情報では暗号化せずに記録し、上記暗号化データ部では上記コンテンツのデータを上記第1の情報と第2の情報とを関連させて暗号化して記録すると共に、上記暗号化されたデータを復号するための上記第1の情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生装置であって、

上記付加情報から暗号化したデータを復号するための第1の情報の少なくとも一部を抜き出す手段と、

上記暗号化したデータを復号するための第1の情報及び

／又は上記第2の情報を使って、上記コンテンツのデータを復号化する手段とを備えるようにしたデータ再生装置。

【請求項125】 コンテンツのデータを少なくとも第1の情報では暗号化せずに記録する平文データ部と、上記コンテンツのデータを少なくとも第1の情報の一部を使って暗号化して記録する暗号化データ部とを設け、上記平文データ部では上記コンテンツのデータを第2の情報で暗号化して記録し、上記暗号化データ部では上記コンテンツのデータを少なくとも上記第1の情報及び／又は第2の情報で暗号化して記録すると共に、上記第1の情報で暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生装置であって、上記平文データ部のデータを第2の情報を使って復号化する手段と、
上記付加情報から暗号化したデータを復号するための第1の情報の少なくとも一部を抜き出す手段と、
上記暗号化したデータを復号するための第1の情報及び／又は上記第2の情報を使って、上記コンテンツのデータを復号化するようにしたデータ再生装置。

【請求項126】 上記付加情報には、コピー管理情報及び／又は再生管理情報を含めるようにし、上記コピー管理情報及び／又は再生管理情報を使って、コピーや再生の管理を行うようにした請求項123、請求項124、又は請求項125に記載のデータ再生装置。

【請求項127】 上記第2の情報で暗号化したデータを復号するための情報は、サブコードの領域から得るようにした請求項124又は請求項125に記載のデータ再生装置。

【請求項128】 上記第2の情報で暗号化したデータを復号するための情報は、リードインのデータから得るようにした請求項124又は請求項125に記載のデータ再生装置。

【請求項129】 上記第2の情報で暗号化したデータを復号するための情報は、TOC (Table Of Contents) のデータから得るようにした請求項124又は請求項125に記載のデータ再生装置。

【請求項130】 上記第2の情報で暗号化したデータを復号するための情報は、トラック又はピットのウォブルデータから得るようにした請求項124又は請求項125に記載のデータ再生装置。

【請求項131】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、
上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生方法

であって、
上記付加情報から暗号化したデータを復号するための情報の少なくとも一部を抜き出し、
上記暗号化したデータを復号するための情報を使って、
上記コンテンツのデータを復号化するようにしたデータ再生装置。

【請求項132】 上記無情報データ部には、無音に相当するオーディオデータを記録するようにした請求項131に記載のデータ再生装置。

10 【請求項133】 上記無情報データ部には、固定パターンに相当するビデオデータを記録するようにした請求項131に記載のデータ再生装置。

【請求項134】 上記無情報データ部には、ランダムパターンに相当するビデオデータを配置するようにした請求項131に記載のデータ再生装置。

20 【請求項135】 コンテンツのデータに平文データ部と暗号化データ部とを設け、
上記平文データ部では上記コンテンツのデータを暗号化せず、上記暗号化データ部では上記コンテンツのデータを暗号化しておき、

上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信するようにしたデータ送信方法。

【請求項136】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、
上記暗号化データ部では上記コンテンツのデータを暗号化しておき、

30 上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信するようにしたデータ送信方法。

【請求項137】 コンテンツのデータに平文データ部と暗号化データ部とを設け、
上記平文データ部では上記コンテンツのデータを暗号化せず、上記暗号化データ部では上記コンテンツのデータを暗号化する手段と、

40 上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信する手段とからなるようにしたデータ送信装置。

【請求項138】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、
上記暗号化データ部では上記コンテンツのデータを暗号化する手段と、

50 上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信する手段とからなるようにしたデータ送信装置。

【請求項139】 コンテンツのデータに平文データ部と暗号化データ部とを設け、
 上記平文データ部では上記コンテンツのデータを暗号化せず、上記暗号化データ部では上記コンテンツのデータを暗号化して送信すると共に、
 上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信されてきたデータを受信するデータ受信方法であって、
 上記平文データ部で送信されている上記コンテンツのデータを再生すると共に、上記平文データ部における上記コンテンツのデータに上記付加情報として埋め込まれている暗号化したデータを復号するための情報を抜き出し、
 上記暗号化したデータを復号するための情報を使って、上記暗号化データ部に暗号化されて送信されてきた上記コンテンツのデータを復号化し、
 上記暗号化データ部に送信されてきたコンテンツのデータを再生するようにしたデータ受信方法。
 【請求項140】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、
 上記暗号化データ部では上記コンテンツのデータを暗号化しておき、
 上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信されてきたデータを受信するデータ受信方法であって、
 上記無情報データ部に上記付加情報として埋め込まれている暗号化したデータを復号するための情報を抜き出し、
 上記暗号化したデータを復号するための情報を使って、上記暗号化データ部に暗号化されて送信されてきた上記コンテンツのデータを復号化し、
 上記暗号化データ部に送信されてきたコンテンツのデータを再生するようにしたデータ受信方法。
 【請求項141】 コンテンツのデータに平文データ部と暗号化データ部とを設け、
 上記平文データ部では上記コンテンツのデータを暗号化せず、上記暗号化データ部では上記コンテンツのデータを暗号化して送信すると共に、
 上記暗号化したデータを復号するための情報の少なくとも一部を、上記平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信されてきたデータを受信するデータ受信装置であって、
 上記平文データ部で送信されている上記コンテンツのデータを再生する手段と、
 上記平文データ部における上記コンテンツのデータに上記付加情報として埋め込まれている暗号化したデータを復号するための情報を抜き出す手段と、

上記暗号化したデータを復号するための情報を使って、
 上記暗号化データ部に暗号化されて送信されてきた上記コンテンツのデータを復号化する手段と、
 上記暗号化データ部に送信されてきたコンテンツのデータを再生する手段とを備えるようにしたデータ受信装置。
 【請求項142】 コンテンツのデータを暗号化して記録する暗号化データ部と、上記暗号化データ部に先行する無情報データ部とを設け、
 上記暗号化データ部では上記コンテンツのデータを暗号化しておき、
 上記無情報データ部に、上記暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信されてきたデータを受信するデータ受信装置であって、
 上記無情報データ部に埋め込まれている暗号化したデータを復号するための情報を抜き出す手段と、
 上記暗号化したデータを復号するための情報を使って、上記暗号化データ部に暗号化されて送信されてきた上記コンテンツのデータを復号化する手段と、
 上記暗号化データ部に送信されてきたコンテンツのデータを再生する手段とを備えるようにしたデータ受信装置。
 【発明の詳細な説明】
 【0001】
 【発明の属する技術分野】この発明は、ビデオデータやオーディオデータのようなコンテンツデータ、コンテンツのデータを記録したデータ記録媒体、データ記録方法及び装置、データ再生方法及び装置、データ送信方法及び装置、データ受信方法及び装置に関するもので、特に、コンテンツのデータ保護に係わる。
 【0002】
 【従来の技術】オーディオコンテンツやビデオコンテンツのデータを記録媒体に記録する際に、著作権の保護を目的として、付加情報としてコピー管理情報をコンテンツのデータに重畳して埋め込むようにしたウォーターマークの開発が進められている。このようなウォーターマークとしては、信号の下位ビットや圧縮時の高次係数に付加情報を挿入する方法、マスキング効果を利用してコンテンツに影響が生じないように付加情報を挿入する方法、スペクトラム拡散を用いて付加情報のスペクトラムを分散させてコンテンツのデータに重畳する方法、所定範囲の第1のピーク若しくは第2のピーク又はその近傍に挿入する方法等が知られている。
 【0003】このようなウォーターマークに、コピー禁止や許可等の情報をいれておけば、コピー禁止等をウォーターマークの情報により管理することができ、著作権の保護の観点から、非常に有用である。また、このようなウォーターマークの情報の中には、デジタルデータのままコピーしたときのみならず、アナログ的にコピーした場

合にもウォーターマークの情報が残っているものもあり、アナログコピーの場合の著作権情報の保護にも有効である。

【0004】

【発明が解決しようとする課題】ところが、ウォーターマークの情報を検出するためには、再生機器側に、ウォーターマーク検出用のためのデコーダが必要になる。再生機器側にウォーターマーク検出のためのデコーダを設けると、回路規模が増大し、コストアップになる。また、ウォーターマークによる著作権の管理情報は、著作権を保護する目的としては重要であるが、コンテンツを利用するユーザ側にとっては、必ずしも重要な情報とはいえない。このことから、記録媒体に記録されるコンテンツのデータにウォーターマークを重畳しても、ユーザの再生機器側では、ウォーターマークの検出が行われず、これにより、著作権が守られなくなる可能性がある。

【0005】また、コンテンツのデータ中には、ユーザに必ず知らせておきたい情報が含まれている場合がある。例えば、映画のビデオデータのコンテンツに、そのコンテンツを提供している企業のコマーシャルが含まれている場合がある。

【0006】ところが、従来では、多くのユーザは、再生時に、そのコマーシャルの部分スキップしてしまう。そのコンテンツを提供している企業側にとすると、コマーシャルの部分スキップされてしまうと、そのコマーシャルの効果が十分に得られず、コマーシャルのために支払った宣伝広告費が回収できない。

【0007】また、映画のようなコンテンツでは、最初に、著作権に関する注意事項の画面が表示される。コンテンツを再生するに当たって、これらの事項は、ユーザに必ず知らせておく必要がある。

【0008】ところが、通常、多くのユーザは、このような事項が示されている画面をスキップしてしまい、著作権や複製に関する禁止事項等の確認が徹底できない。

【0009】したがって、この発明の目的は、コピー禁止や再生禁止等の著作権の保護に関する情報がウォーターマークとして記録されている場合に、再生時に、このウォーターマークの情報が確実にデコードされるようにして、著作権の保護が図れるようにしたコンテンツデータ、データ記録媒体、データ記録方法及び装置、データ再生方法及び装置、データ送信方法及び受信方法を提供することにある。

【0010】この発明の他の目的は、ユーザに知らせたい部分が確実に再生されるようにしたコンテンツデータ、データ記録媒体、データ記録方法及び装置、データ再生方法及び装置、データ送信方法及び装置、データ受信方法及び装置を提供することにある。

【0011】

【課題を解決するための手段】請求項1の発明は、コンテンツのデータを暗号化せずに配置する平文データ部

と、コンテンツのデータを暗号化して配置する暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せずに配置し、暗号化データ部ではコンテンツのデータを暗号化して配置すると共に、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたコンテンツデータである。

【0012】請求項2の発明は、コンテンツのデータを少なくとも第1の情報では暗号化せずに配置する平文データ部と、コンテンツのデータを少なくとも第1の情報の一部を使って暗号化して配置する暗号化データ部とを設け、平文データ部ではコンテンツのデータを少なくとも第1の情報では暗号化せずに配置し、暗号化データ部ではコンテンツのデータを第1の情報と第2の情報とを関連させて暗号化して配置すると共に、暗号化されたデータを復号するための第1の情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたコンテンツデータである。

【0013】請求項3の発明は、コンテンツのデータを少なくとも第1の情報では暗号化せずに配置する平文データ部と、コンテンツのデータを少なくとも第1の情報の一部を使って暗号化して配置する暗号化データ部とを設け、平文データ部ではコンテンツのデータを第2の情報で暗号化して配置し、暗号化データ部ではコンテンツのデータを少なくとも第1の情報及び／又は第2の情報で暗号化して配置すると共に、第1の情報で暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたコンテンツデータである。

【0014】請求項21の発明は、コンテンツのデータを暗号化して配置する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、平文データ部にはコンテンツのデータを暗号化せずに配置し、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたコンテンツデータである。

【0015】請求項25の発明は、コンテンツのデータを暗号化せずに記録する平文データ部と、コンテンツのデータを暗号化して記録する暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せずに記録し、暗号化データ部ではコンテンツのデータを暗号化して記録すると共に、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体である。

【0016】請求項26の発明は、コンテンツのデータを少なくとも第1の情報では暗号化せずに記録する平文データ部と、コンテンツのデータを少なくとも第1の情報の一部を使って暗号化して記録する暗号化データ部とを設け、平文データ部ではコンテンツのデータを少なく

報で暗号化して記録すると共に、第1の情報で暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録方法である。

【００２２】請求項７９の発明は、コンテンツのデータを暗号化して記録する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録方法である。

【００２３】請求項８３の発明は、コンテンツのデータを暗号化せずに記録する平文データ部と、コンテンツのデータを暗号化して記録する暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せずに記録し、暗号化データ部ではコンテンツのデータを暗号化して記録する手段と、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込む手段とを備えるようにしたデータ記録装置である。

【００２４】請求項８４の発明は、コンテンツのデータを少なくとも第１の情報では暗号化せずに記録する平文データ部と、コンテンツのデータを少なくとも第１の情報の一部を使って暗号化して記録する暗号化データ部とを設け、平文データ部ではコンテンツのデータを少なくとも第１の情報では暗号化せずに記録し、暗号化データ部ではコンテンツのデータを第１の情報と第２の情報とを関連させて暗号化して記録する手段と、暗号化されたデータを復号するための第１の情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込む手段とを備えるようにしたデータ記録装置である。

【 0 0 2 5 】 請 求 項 8 5 の 発 明 は、 コ ン テ ン ツ の デ ー タ
を 少 な く と も 第 1 の 情 報 で は 暗 号 化 せ ず に 記 録 す る 平 文
デ ー タ 部 と、 コ ン テ ン ツ の デ ー タ を 少 な く と も 第 1 の 情
報 の 一 部 を 使 っ て 暗 号 化 し て 記 録 す る 暗 号 化 デ ー タ 部 と
を 設 け、 平 文 デ ー タ 部 で は コ ン テ ン ツ の デ ー タ を 第 2 の
情 報 で 暗 号 化 し て 記 録 し、 暗 号 化 デ ー タ 部 で は コ ン テ ン
ツ の デ ー タ を 少 な く と も 第 1 の 情 報 及 び／又 は 第 2 の 情
報 で 暗 号 化 し て 記 録 す る 手 段 と、 第 1 の 情 報 で 暗 号 化 し
た デ ー タ を 復 号 す る た め の 情 報 の 少 な く と も 一 部 を、 平
文 デ ー タ 部 お け る コ ン テ ン ツ の デ ー タ に 付 加 情 報 と し
て 埋 め 込 む 手 段 と を 備 え る よ う に し た デ ー タ 記 録 装 置 で
あ る。

【００２６】請求項１０７の発明は、コンテンツのデータを暗号化して配置する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録装置である。

【００２７】請求項１１１の発明は、コンテンツのデー

録媒体を再生するデータ再生方法であって、付加情報から暗号化したデータを復号するための情報の少なくとも一部を抜き出し、暗号化したデータを復号するための情報を使って、コンテンツのデータを復号化するようにしたデータ再生方法である。

【 0 0 3 1 】 請求項 1 2 3 の発明は、コンテンツのデータを暗号化せずに記録する平文データ部と、コンテンツのデータを暗号化して記録する暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せずに記録し、暗号化データ部ではコンテンツのデータを暗号化して記録すると共に、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生装置であって、付加情報から暗号化したデータを復号するための情報の少なくとも一部を抜き出す手段と、暗号化したデータを復号するための情報を使って、コンテンツのデータを復号化する手段とを備えるようにしたデータ再生装置である。

20 【 0 0 3 2 】 請求項 1 2 4 の発明は、コンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録する平文データ部と、コンテンツのデータを少なくとも第 1 の情報の一部を使って暗号化して記録する暗号化データ部とを設け、平文データ部ではコンテンツのデータを少なくとも第 1 の情報では暗号化せずに記録し、暗号化データ部ではコンテンツのデータを第 1 の情報と第 2 の情報とを関連させて暗号化して記録すると共に、暗号化されたデータを復号するための第 1 の情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生装置であって、付加情報から暗号化したデータを復号するための第 1 の情報の少なくとも一部を抜き出す手段と、暗号化したデータを復号するための第 1 の情報及び／又は第 2 の情報を使って、コンテンツのデータを復号化する手段とを備えるようにしたデータ再生装置である。

【0033】請求項125の発明は、コンテンツのデータを少なくとも第1の情報では暗号化せずに記録する平文データ部と、コンテンツのデータを少なくとも第1の情報の一部を使って暗号化して記録する暗号化データ部とを設け、平文データ部ではコンテンツのデータを第2の情報で暗号化して記録し、暗号化データ部ではコンテンツのデータを少なくとも第1の情報及び／又は第2の情報で暗号化して記録すると共に、第1の情報で暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生装置であって、平文データ部のデータを第2の情報を使って復号化する手段と、付加情報から暗号化したデータを復号するための第1の情報の少なくとも一部を

抜き出す手段と、暗号化したデータを復号するための第1の情報及び／又は第2の情報を使って、コンテンツのデータを復号化するようにしたデータ再生装置である。

【0034】請求項131の発明は、コンテンツのデータを暗号化して記録する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込むようにしたデータ記録媒体を再生するデータ再生方法であって、付加情報から暗号化したデータを復号するための情報の少なくとも一部を抜き出し、暗号化したデータを復号するための情報を使って、コンテンツのデータを復号化するようにしたデータ再生装置である。

【0035】請求項135の発明は、コンテンツのデータに平文データ部と暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せず、暗号化データ部ではコンテンツのデータを暗号化しておき、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信するようにしたデータ送信方法である。

【0036】請求項136の発明は、コンテンツのデータを暗号化して記録する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、暗号化データ部ではコンテンツのデータを暗号化しておき、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信するようにしたデータ送信方法である。

【0037】請求項137の発明は、コンテンツのデータに平文データ部と暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せず、暗号化データ部ではコンテンツのデータを暗号化する手段と、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信する手段とからなるようにしたデータ送信装置である。

【0038】請求項138の発明は、コンテンツのデータを暗号化して記録する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、暗号化データ部ではコンテンツのデータを暗号化する手段と、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信する手段とからなるようにしたデータ送信装置である。

【0039】請求項139の発明は、コンテンツのデータに平文データ部と暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せず、暗号化データ部ではコンテンツのデータを暗号化して送信すると共に、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信されてきたデータを受信

するデータ受信方法であって、平文データ部で送信されているコンテンツのデータを再生すると共に、平文データ部におけるコンテンツのデータに付加情報として埋め込まれている暗号化したデータを復号するための情報を抜き出し、暗号化したデータを復号するための情報を使って、暗号化データ部に暗号化されて送信されてきたコンテンツのデータを復号化し、暗号化データ部に送信されてきたコンテンツのデータを再生するようにしたデータ受信方法である。

10 【0040】請求項140の発明は、コンテンツのデータを暗号化して記録する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、暗号化データ部ではコンテンツのデータを暗号化しておき、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信されてきたデータを受信するデータ受信方法であって、無情報データ部に付加情報として埋め込まれている暗号化したデータを復号するための情報を抜き出し、暗号化したデータを復号するための情報を使って、暗号化データ部に暗号化されて送信されてきたコンテンツのデータを復号化し、暗号化データ部に送信されてきたコンテンツのデータを再生するようにしたデータ受信方法である。

20 【0041】請求項141の発明は、コンテンツのデータに平文データ部と暗号化データ部とを設け、平文データ部ではコンテンツのデータを暗号化せず、暗号化データ部ではコンテンツのデータを暗号化して送信すると共に、暗号化したデータを復号するための情報の少なくとも一部を、平文データ部におけるコンテンツのデータに付加情報として埋め込んで送信されてきたデータを受信するデータ受信装置であって、平文データ部で送信されているコンテンツのデータを再生する手段と、平文データ部におけるコンテンツのデータに付加情報として埋め込まれている暗号化したデータを復号するための情報を抜き出す手段と、暗号化したデータを復号するための情報を使って、暗号化データ部に暗号化されて送信されてきたコンテンツのデータを復号化する手段と、暗号化データ部に送信されてきたコンテンツのデータを再生する手段とを備えるようにしたデータ受信装置である。

30 【0042】請求項142の発明は、コンテンツのデータを暗号化して記録する暗号化データ部と、暗号化データ部に先行する無情報データ部とを設け、暗号化データ部ではコンテンツのデータを暗号化しておき、無情報データ部に、暗号化したデータを復号するための情報の少なくとも一部を付加情報として埋め込んで送信されてきたデータを受信するデータ受信装置であって、無情報データ部に埋め込まれている暗号化したデータを復号するための情報を抜き出す手段と、暗号化したデータを復号するための情報を使って、暗号化データ部に暗号化されて送信されてきたコンテンツのデータを復号化する手段と、暗号化データ部に送信されてきたコンテンツのデー

タを再生する手段とを備えるようにしたデータ受信装置である。

【0043】コンテンツのファイルには、コンテンツのデータを暗号化せずに記録する平文データ部と、コンテンツのデータを暗号化して記録する暗号化データ部とが設けられ、平文データ部では、コンテンツのデータが暗号化せずに記録され、暗号化データ部ではコンテンツのデータが暗号化されて記録される。そして、暗号化のための鍵の少なくとも一部が平文データ部におけるコンテンツのデータに付加情報として埋め込まれている。

【0044】再生時には、平文データ部のコンテンツのデータに重畳されて記録されているウォータマークに含まれるキー情報を使用して、それに続く暗号化部のデータの復号化処理が行われる。

【0045】このため、ウォータマークの情報を検出しないと、暗号化データ部のデータが再生できなくなるため、ウォータマークの情報が必ず再生される。よって、ウォータマークに含まれているコピーや再生を管理するための情報が必ず得られるようになり、ウォータマークによる著作権の管理が確実に行われるようになる。

【0046】また、暗号化のための鍵情報を含むウォータマークが埋め込まれる平文データ部に、ユーザに必ず知らせておきたい情報を記録しておく、ユーザは、この必ず知らせておきたい情報を再生しなければ、暗号化データ部のコンテンツを復号して再生することができなくなる。

【0047】したがって、平文データ部に、著作権や複製に関する禁止事項の画面を記録しておけば、ユーザがこの画面を見なければコンテンツの映像データを再生できないことになり、著作権や複製に関する禁止事項等をユーザに確認させることができる。また、平文データ部にコマーシャルを記録しておく、ユーザは、コマーシャルを見なければ、コンテンツの映像データを再生できなくなることになり、コマーシャルを確実に見せることができ、コマーシャルの提供の不利益がなくなる。

【0048】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。図1は、この発明が適用された記録媒体におけるコンテンツのデータのファイル構成を示すものである。なお、ここで、コンテンツとしては、音楽データ、動画データ、画像データ、ゲームのデータ等が考えられる。

【0049】図1Aにおいて、コンテンツのデータのファイルには、先頭にヘッダH1が設けられ、これに続いて、平文データ部A1、暗号化データ部B1、平文データ部A2、暗号化データ部B2、…が設けられる。

【0050】平文データ部A1、A2、…には、コンテンツのデータD1、D3、…が記録される。この平文データ部A1、A2、…に記録されるコンテンツのデータD1、D3、…は、暗号化されていない、所謂平文のデ

ータである。

【0051】暗号化データ部B1、B2、…には、コンテンツのデータD2e、D4e、…が記録される。このコンテンツのデータD2e、D4e、…は、コンテンツのデータD2、D4、…を暗号化したものである。

【0052】これと共に、平文データ部A1、A2、…には、ウォータマーク情報WM1、WM3、…がこのコンテンツデータD1、D3に重畳されて記録される。暗号化データ部B1、B2、…には、ウォータマークWM2、WM4…がコンテンツのデータD2e、D4eに重畳されて記録される。

【0053】ウォータマークWM1、WM2、WM3…には、コピー管理情報や再生管理情報等が含まれる。更に、平文データ部A1、A2、…のウォータマークWM1、WM3…には、平文データ部A1、A2、…の夫々に続く暗号化データ部B1、B2、…のコンテンツのデータD2e、D4e、…の暗号を復号するためのキー情報Ka、Kb、…が含まれている。

【0054】再生時には、まず、平文データ部A1のコンテンツのデータD1が再生される。これと共に、このコンテンツのデータD1に重畳されているウォータマークWM1が検出され、このウォータマークWM1に含まれているキー情報Kaが取り出される。

【0055】それから、暗号化データ部B1のコンテンツのデータD2eの再生が行われる。このとき、図1Bに示すように、平文データ部A1のコンテンツのデータD1に重畳されて記録されているウォータマークWM1に含まれるキー情報Kaを使用して、コンテンツのデータD2eの暗号の復号化処理が行われる。

【0056】次に、平文データ部A2のコンテンツのデータD3が再生される。これと共に、このコンテンツのデータD3に重畳されているウォータマークWM3が検出される。そして、このウォータマークWM3に含まれているキー情報Kbが取り出される。

【0057】それから、暗号化データ部B2のコンテンツのデータD4eの再生が行われる。このとき、図2Bに示すように、平文データ部A2のコンテンツのデータD3に重畳されて記録されているウォータマークWM3に含まれるキー情報Kbを使用して、コンテンツのデータD4eの暗号の復号化処理が行われる。

【0058】このように、この発明の一実施の形態では、コンテンツのデータのファイルに、平文データ部A1、A2、…と、暗号化データ部B1、B2、…とが設けられ、平文データ部A1、A2、…には、コンテンツのデータが暗号化されずに記録され、暗号化データ部B1、B2、…には、コンテンツのデータが暗号化されて記録される。そして、平文データ部A1、A2、…のコンテンツのデータのウォータマークWM1、WM3、…の中には、これに続く暗号化データ部B1、B2、…のコンテンツのデータの暗号を解読するためのキー情報K

a、K b、…が含まれている。

【0059】したがって、図1に示すようなファイル構成としておくと、このファイルのコンテンツのデータを再生する際には、平文データ部A 1、A 2、…のコンテンツのデータに重畳されているウォータマークWM 1、WM 3、…の情報を検出し、このウォータマークWM 1、WM 3、…の情報中のキー情報K a、K b、…を使って、暗号化データ部B 1、B 2、…のコンテンツのデータの暗号の復号化を行う必要があり、ウォータマークの情報が必ず復号されるようになる。

【0060】ウォータマークには、例えば、コピーを管理する情報や、再生を管理する情報が記録される。このように、この発明の実施の形態では、ウォータマークの情報を検出しないと、暗号化データ部のデータが再生できなくなるため、ウォータマークの情報が必ず再生される。よって、ウォータマークに含まれているコピーや再生を管理するための情報が必ず得られるようになり、ウォータマークによる著作権の管理が確実に行われるようになる。

【0061】なお、ウォータマークとしては、スペクトラム拡散し、コンテンツのデータに重畳するものや、信号のピーク値を検出し、コンテンツのデータに影響を与えないように、ピーク値にウォータマークを挿入するものや、コンテンツの下位ビットにウォータマークの情報を挿入するものや、圧縮時の高次係数にウォータマークの情報を挿入するもの等、種々のものが提案されている。これらのうち、どのようなウォータマークを用いても良い。

【0062】また、1ファイル中に、どの部分を平文データ部とし、どの部分を暗号化データ部にするか、平文データ部や暗号化データ部の長さ、平文データ部や暗号化データ部の数は、特に限定する必要はない。

【0063】平文データ部のウォータマークのキー情報を使って暗号化部のデータの暗号の復号化を行うことを考えると、暗号化部に先行して平文データ部を設けると処理が簡単である。

【0064】特に、ファイルの先頭部分だけ平文データ部にしておき、これに続く部分は全て暗号化データ部にしておき、ファイルの先頭の平文データ部のウォータマークに、それに続く暗号化部分の暗号を復号化するためのキー情報を入れておくと、処理が簡単である。

【0065】しかしながら、暗号化データ部の後に平文データ部を設け、再生時に、平文データ部を先に読むようにしても良く、必ずしも、暗号化部に先行して平文データ部を設ける必要はない。

【0066】図2は、ウォータマークを挿入するためのエンコーダの一例である。この例は、コンテンツのデータの下位ビットにウォータマークの情報を挿入するものである。そして、この例では、ウォータマークの情報の成分を、聴感上、影響のない帯域に入れるようにしてい

る。

【0067】図2において、入力端子1にオリジナルデータが供給される。入力端子2にウォータマークのデータが供給される。

【0068】入力端子2からのウォータマークのデータは、ランダムマイザ3に供給される。ランダムマイザ3で、ウォータマークのデータが白色ノイズ化される。ランダムマイザ3の出力が減算回路4に供給されると共に、加算回路5に供給される。

10 【0069】入力端子1からのデータは、減算回路6に供給される。減算回路6の出力が減算回路4に供給されると共に、減算回路7に供給される。減算回路4の出力が量子化回路8に供給される。量子化回路8の出力が加算回路5に供給される。

【0070】加算回路5で、量子化回路8の出力と、ランダムマイザ3の出力とが加算される。加算回路5の出力が出力端子11から出力されると共に、減算回路7に供給される。減算回路7で、加算回路5の出力から加算回路6の出力が減算される。

20 【0071】減算回路7の出力がノイズシェープフィルタ10に供給される。ノイズシェープフィルタ10の出力が減算回路6に供給される。減算回路6で、入力端子1からのデータから、ノイズシェープフィルタ10の出力が減算される。

【0072】図2に示すようなウォータマークエンコーダは、データの下位ビットにウォータマークのデータを挿入するものである。そして、コンテンツのデータにウォータマークを挿入したことによる影響が出ないように、ノイズ成分を聴感上問題のない所に、入れるようにしている。

30 【0073】つまり、図2において、入力端子1からのデータは、量子化回路8で量子化される。加算回路5により、この量子化回路8から出力されるデータの下位ビットに、ランダムマイザ3からのウォータマークのデータが挿入される。

【0074】量子化回路8の前段には、減算回路4が設けられる。そして、減算回路4において、入力端子1からのデータから、ウォータマークのデータが減じられる。このように、量子化回路8の前段において、入力端子1からのデータからウォータマークのデータが減じられる。これにより、量子化回路8の後段の加算回路5で、コンテンツのデータに対してウォータマークのデータが挿入されることの影響が除かれる。

50 【0075】加算回路5からは、ウォータマークのデータが付加されたデータが出力される。この加算回路5の出力は出力端子11から出力される。これと共に、減算回路7で、加算回路5の出力データと、減算回路6の出力データとが減算される。この減算回路7により、量子化回路8からの出力データと、量子化回路8への入力データとが減算されることになり、量子化に伴うノイズ成

分が取り出される。このノイズ成分は、ノイズシェーブフィルタ 10 により聴感上問題のない所に移され、減算回路 6 に供給される。

【0076】図 3 は、上述のようにして挿入されたウォータマークの情報をデコードするウォータマークのデコーダの一例である。

【0077】図 3 において、入力端子 21 に、上述のようにしてウォータマークが重畳されたコンテンツのデータが供給される。入力端子 21 からのデータが量子化回路 22 に供給される。量子化回路 22 の出力が出力端子 23 から出力されると共に、下位ビット抜き出し回路 24 に供給される。

【0078】下位ビット抜き出し回路 24 により、データの下位ビットに挿入されているウォータマークのデータが取り出される。このウォータマークのデータは、逆ランダムマイザ 25 に供給される。

【0079】逆ランダムマイザ 25 は、前述のエンコーダにおけるランダムマイザ 3 と対応する処理を行うものである。逆ランダムマイザ 25 により、ランダム化されていたウォータマークの情報が元の状態に戻される。この逆ランダムマイザ 25 から、ウォータマークの情報が得られる。このウォータマークの情報が出力端子 26 から出力される。

【0080】図 4 は、図 1 に示したように、平文データ部と暗号化データ部とを設け、平文データ部のウォータマークの情報に、それに続く暗号化データ部のデータの暗号を復号するためのキー情報を含めるように、コンテンツのファイルを記録媒体に記録するような記録装置の一例である。また、この例では、記録媒体として、CD-R (Compact Disc Recordable) や CD-RW (Compact Disc Rewritable) 或いは CD2-R や CD2-RW のような光ディスクが用いられる。

【0081】図 4 に示す記録装置において、入力端子 51 に、コンテンツのデータが供給される。このコンテンツのデータは、入力端子 51 から、ウォータマーク付加回路 53 に供給される。

【0082】入力端子 52 に、ウォータマークデータが供給される。このウォータマークデータは、入力端子 52 から、ウォータマーク生成回路 54 に供給される。このウォータマークデータには、コピー管理情報や再生管理情報が含まれると共に、平文データに続く暗号化データ部のコンテンツのデータの暗号解読をするためのキー情報が含まれている。このウォータマーク生成回路 54 の出力がウォータマーク付加回路 53 に供給される。

【0083】ウォータマーク付加回路 53 で、入力端子 51 からのコンテンツのデータにウォータマークの情報が付加される。

【0084】なお、ウォータマークとしては、ウォータマークの情報をスペクトラム拡散し、コンテンツのデータに重畳するようなものや、信号のピーク値を検出し、

コンテンツのデータに影響を与えないように、ピーク値にウォータマークを挿入するものや、コンテンツの下位ビットにウォータマークの情報を挿入するものや、圧縮時の高次係数にウォータマークの情報を挿入するもの等、どのようなウォータマークを用いても良い。

【0085】ウォータマーク付加回路 53 の出力がスイッチ回路 55 に供給される。スイッチ回路 55 は、平文／暗号データ切換信号発生回路 56 の出力により、平文データ部と暗号化データ部とに応じて切り換えられる。

10 【0086】平文データ部では、スイッチ回路 55 は端子 55A 側に設定される。これにより、入力端子 51 からのコンテンツのデータは、ウォータマーク付加回路 53 でウォータマークのデータが付加され、スイッチ回路 55 を介して、マルチプレクサ 57 に供給される。なお、このとき、ウォータマーク付加回路 54 からは、ウォータマークデータとして、コピー管理情報や再生管理情報が出力されると共に、平文データ部に続く暗号化データ部のコンテンツのデータの暗号解読をするためのキー情報が出力される。

20 【0087】暗号化データ部では、スイッチ回路 55 は端子 55B 側に設定される。これにより、入力端子 51 からのコンテンツのデータは、ウォータマーク付加回路 53 でウォータマークが付加され、スイッチ回路 55 を介して、暗号化回路 58 に供給される。暗号化回路 58 には、ウォータマーク生成回路 54 から暗号キーが送られる。また、暗号化回路 58 には、キー生成回路 59 から、暗号キーが送られる。

30 【0088】このように、この例では、ウォータマーク生成回路 54 から出力され、ウォータマークの情報に格納される第 1 の暗号キーを使ってコンテンツのデータが暗号化されると共に、キー発生回路 59 から出力される第 2 の暗号キーを使ってコンテンツのデータが暗号化される。キー発生回路 59 からの第 2 のキー情報を復号化するための情報は、ディスクのリードインや、トラッキング方向のウォブルデータ、サブコードのデータ、TOC (Table Of Contents) データとして記録される。

40 【0089】このように、2 系列の暗号化を行うことで、より強力な管理を行える。また、ウォータマークの情報は書き換えが困難であり、ディスクのリードインや、サブコードのデータ、TOC データ等は書き換えが可能であることから、この暗号化は、ユーザ毎に使用することが考えられる。

50 【0090】また、コンテンツファイル全体を暗号化したい場合には、平文データ部でも暗号化データ部でもスイッチ回路 55 を端子 55B 側に設定し、平文データ部では、キー発生回路 59 からの第 2 の暗号キーで暗号化を行い、暗号化データ部では、ウォータマーク生成回路 54 からの第 1 の暗号キーとキー発生回路 59 からの第 2 の暗号キーとで二重に暗号化を行うようにしても良い。

【0091】また、平文データ部でのみ、キー発生回路59からの第2の暗号キーで暗号化を行うようにしても良い。この場合、キー発生回路59からの第2の暗号キーで、コンテンツのデータとそこに付加されているウォータマークも暗号化される。このウォータマークには、第1の暗号を復号するための情報が含まれている。このため、第2の暗号を復号することで、ウォータマークの情報が復号され、このウォータマークの情報から第1の暗号化を復号するための情報が抽出されて、暗号化データ部のデータが復号される。

【0092】また、第1の暗号キーと第2の暗号キーとを関連させて、暗号化を行ったり、更に、他の暗号キーとを関連させるようにしても良い。例えば、第1の暗号キーと第2の暗号キーとから暗号キーを生成し、この暗号キーで暗号データ部のコンテンツのデータを暗号化するようにしても良い。

【0093】暗号化回路58で、暗号化データ部のコンテンツのデータは、ウォータマーク生成回路54からの暗号キーと、キー発生回路59からの暗号キーにより暗号化される。この暗号化されたデータは、マルチプレクサ57に供給される。

【0094】マルチプレクサ57の出力がエラー訂正符号化回路60に供給される。エラー訂正符号化回路60で、エラー訂正符号化処理が行われる。エラー訂正回路60の出力データは、変調回路61に供給される。変調回路61の出力は、記録アンプ62を介して、光学ピックアップ63に供給され、このデータが光ディスク64に記録される。

【0095】また、キー発生回路59からのキー情報は、記録回路65に供給される。記録回路65は、ディスクのリードインのデータ記録や、トラッキング方向にウォブルされデータの記録やTOCの記録を行うものである。

【0096】なお、平文データ部と暗号化データ部とを光ディスクに記録する場合に、光ディスクを外周側の記録領域と内周側の記録領域とに分割し、各記録領域で、平文データ部と暗号データ部とを分けるようにしても良い。

【0097】つまり、例えば、CD2では、図5に示すように、ディスクを内周側の領域AR1と外周側の領域AR2とに分けることができる。外周側の領域AR2では、データを倍密度で記録することができる。このようなCD2のディスクの場合には、内周側の領域AR1が平文データ部とされ、外周側の領域AR2が暗号化データ部とされる。

【0098】光ディスクの内周側の領域AR1には、コンテンツのデータが平文で記録されていると共に、暗号化のため鍵の少なくとも一部がウォータマークとして埋め込まれている。光ディスクの外周側の領域AR2には、コンテンツデータが暗号化されて記録される。

【0099】再生時には、まず、ディスクの内周側の領域AR1が再生される。そして、このディスクの内周側の平文データ部に記録されているコンテンツのデータが再生されると共に、ウォータマークとして埋め込まれている暗号化のための鍵の情報が読み取られる。それから、ディスクの外周側の領域AR2が再生され、領域AR2に記録されている暗号化されたコンテンツのデータが読み出される。この領域AR2から再生された暗号化されたコンテンツのデータは、ディスクの内周側の領域AR1のウォータマークから得られた鍵を使って復号される。

【0100】図6は、上述のように、平文データ部と暗号化データ部とを設け、平文データ部のウォータマークの情報に、それに続く暗号化データ部のデータの暗号を復号するためのキー情報を含めるように、コンテンツのファイルを記録した記録媒体を再生する再生装置の一例を示すものである。

【0101】図6において、ディスク71の信号が光学ピックアップ72で再生される。光学ピックアップ72の出力が再生アンプ73を介して、復調回路74に供給される。復調回路74の出力がエラー訂正回路75に供給される。エラー訂正回路75により、エラー訂正処理が行われる。エラー訂正回路75の出力がスイッチ回路76に供給されると共に、ウォータマーク検出回路77に供給される。ウォータマーク検出回路77により、ウォータマークのデータがデコードされる。

【0102】また、光学ピックアップ72の出力がキー情報抽出回路82に供給される。キー情報抽出回路82により、ディスクのリードインや、トラッキング方向のウォブルデータ、サブコードのデータ、TOCに記録されていたキー情報が抽出される。

【0103】スイッチ回路76は、平文／暗号化データ切換回路78により設定される。平文データ部が再生されているときには、スイッチ回路76は端子76A側に設定される。このため、光学ピックアップ71の再生データは、復調回路74で復調され、エラー訂正回路75でエラー訂正処理された後、スイッチ回路76を介して、マルチプレクサ79に供給される。

【0104】暗号化データ部のデータが再生されているときには、端子76B側に設定される。このため、暗号化データ部のデータが再生化されているときには、光学ピックアップ71の再生データは、復調回路74で復調され、エラー訂正回路75でエラー訂正処理された後、スイッチ回路76を介して、暗号データの復号回路80に供給される。

【0105】暗号データの復号回路80には、ウォータマーク検出回路77から、キー情報が供給されると共に、暗号キー抽出回路77から、キー情報が供給される。すなわち、暗号化データ部のデータを復号するためのキー情報は、その前の平文データ部のウォータマーク

のデータに含まれている。ウォータマーク検出回路 77 で、その前の平文データ部のウォータマークのデータが検出され、この中から、キー情報が抽出される。このキー情報がウォータマーク検出回路 77 から暗号の復号化回路 80 に供給される。

【0106】また、ディスクのリードインや、トラッキング方向のウォブルデータ、TOC に暗号化キーが記録されている場合がある。この暗号化キーがキー情報抽出回路 79 で抽出される。このキー情報がキー情報抽出回路 79 から暗号化の復号化回路 80 に供給される。

【0107】復号化回路 80 で、ウォータマーク検出回路 77 からのキー情報と、暗号キー抽出回路 79 からのキー情報とにより、暗号の復号化が行われる。この復号化されたデータは、マルチプレクサ 79 に供給される。マルチプレクサ 79 の出力が出力端子 81 に供給される。この出力端子 81 からは、光ディスク 71 に記録されていたコンテンツのデータの再生出力が得られる。

【0108】なお、上述の例では、平文データ部と暗号データ部とを設けているが、平文データ部を無音や無映像の部分（無情報の部分）に設けるようにしても良い。

【0109】つまり、例えば、コンテンツのデータとしてオーディオ信号を記録した場合、図 7A に示すように、平文データ部（無音データ部）A11 が無音に相当するオーディオデータ（オール「0」）が記録される。この無音に相当するオーディオデータに、暗号化のための鍵情報を含むウォータマークが埋め込まれる。暗号化データ部 B11 には、コンテンツのオーディオデータが暗号化されて記録される。

【0110】再生時には、平文データ部 A11 に埋め込まれている鍵情報が読み取られる。そして、平文データ部 A11 から読み取られた鍵情報を使って、暗号化データ部 B11 に記録されているコンテンツのオーディオデータが復号されて、再生される。

【0111】例えば、1 枚の CD には、通常、複数の曲が記録されており、この曲間には、無音の部分がある。例えば、この曲間の無音部分が平文データ部とされ、ここに、暗号化の鍵情報を含むウォータマークが埋め込まれる。このようにすると、曲間の無音の部分が再生されている間に、この間にウォータマークとして埋め込まれている鍵情報が読み取られ、これに続く音楽が再生されるときに、この鍵情報を使って暗号化されたデータの復号がなされるようになる。

【0112】また、例えば、コンテンツのデータとしてビデオデータとした場合、図 7B に示すように、平文データ部 A21 に、画面ミュートしたときのデータ、例えば、全体が青や黒、白のような固定パターンのデータが記録される。勿論、この固定パターンの画面に、モードの設定状態や警告を示す簡単なキャラクタを含む場合もある。また、無信号時に相当する画面のデータとしても良い。無信号に相当するビデオデータは、再生すると、

スノーノイズのようなランダムパターンの画面である。そして、この平文データ部 A21 のデータに、暗号化のための鍵情報を含むウォータマークが埋め込まれる。暗号化データ部 B21 には、コンテンツのビデオデータが暗号化されて記録されている。

【0113】再生時には、平文データ部 A21 にウォータマーク上として埋め込まれている鍵情報が読み取られる。そして、平文データ部 A21 から読み取られた鍵情報を使って、暗号化データ部 B21 に記録されているコンテンツのデータが復号され、再生される。

【0114】通常、映画のようなビデオコンテンツでは、開始時に、何も記録されていないブルーバックのような画面が現れる。この例では、このコンテンツの開始時のブルーバックのような画面に、暗号化の鍵情報を含むウォータマークが埋め込まれている。このようにすると、コンテンツの最初のブルーバックの部分が再生されている間に、ウォータマークとして埋め込まれている鍵情報が読み取られ、これに続く映画のようなビデオコンテンツが再生されるときに、この鍵情報を使って暗号化されたデータの復号がなされるようになる。

【0115】このように、平文データ部（無音データ部）を、オーディオ信号の場合には無音としたり、ビデオ信号の場合にはブルーバックとした無音データ部とすることで、ウォータマークに付加情報として埋め込まれている情報が必ず再生されるようになると共に、コンテンツのデータを全て暗号化して保護することができるようになる。

【0116】また、このようなデータが記録された記録媒体のコンテンツのデータをコピーする際、無音の部分は不要だとして、無音部分を取り除いてコピーすることが多い。この無音部分には、暗号化データを復号するための鍵情報を含むウォータマークが記録されているので、無音部分を取り除いてコピーが行われると、復号が行えなくなる。このため、不正コピーを防止することができる。

【0117】また、暗号化のための鍵情報を含むウォータマークが埋め込まれる平文データ部に、ユーザに必ず知らせておきたい情報を記録しておく、ユーザは、この必ず知らせておきたい情報を再生しなければ、暗号化データ部のコンテンツを復号して再生することができなくなる。

【0118】例えば、図 8A では、平文データ部 A31 にそのコンテンツの製作者を代表するような画面のビデオデータが記録され、暗号化データ部 B31 に記録されるビデオデータの暗号化の鍵情報を含むウォータマークが埋め込まれる。暗号化データ部 B31 には、コンテンツのビデオデータが暗号化されて記録される。

【0119】図 8B では、平文データ部 A41 に著作権の保護に関する事項の警告を示す画面のビデオデータが記録され、暗号化データ部 B41 に記録されるビデオデ

ータの暗号化の鍵情報を含むウォータマークが埋め込まれる。暗号化データ部B 4 1には、コンテンツのビデオデータが暗号化されて記録される。

【0 1 2 0】図8 Cでは、平文データ部A 5 1にコマーシャルの画面のビデオデータが記録され、暗号化データ部B 5 1に記録されるビデオデータの暗号化の鍵情報を含むウォータマークが埋め込まれる。暗号化データ部B 5 1には、コンテンツのビデオデータが暗号化されて記録される。

【0 1 2 1】図8 Aに示すように、平文データ部A 3 1にそのコンテンツの製作者を代表するような画面のビデオデータが記録されている場合には、図9 Aに示すように、平文データ部A 3 1のコンテンツの製作者を代表するような画面が映し出されている間に、ウォータマークが読み出され、ウォータマークから、これに続くコンテンツの暗号化を復号するためのキー情報が取得される。したがって、ユーザは、図9 Aに示すようなそのコンテンツの製作者を代表するような画面を見なければ、これに続くコンテンツの画面を再生できないことになる。

【0 1 2 2】図8 Bに示すように、平文データ部A 4 1に著作権の保護に関する事項の警告を示す画面のビデオデータが記録されている場合には、図9 Bに示すように、平文データ部A 4 1の著作権の保護に関する事項の警告を示す画面が映し出されている間に、ウォータマークが読み出され、ウォータマークから、これに続くコンテンツの暗号化を復号するためのキー情報が取得される。したがって、ユーザは、図9 Bに示すような著作権の保護に関する事項の警告を示す画面を見なければ、これに続くコンテンツの画面を再生できないことになる。

【0 1 2 3】図8 Cに示すように、平文データ部A 5 1に企業のコマーシャルの画面のビデオデータが記録されている場合には、図9 Cに示すように、平文データ部A 5 1のコマーシャルの画面映し出されている間に、ウォータマークが読み出され、ウォータマークから、これに続くコンテンツの暗号化を復号するためのキー情報が取得される。したがって、ユーザは、図9 Cに示すようなコマーシャルの画面を見なければ、これに続くコンテンツの画面を再生できないことになる。

【0 1 2 4】例えば、映画のコンテンツには、著作権者の情報や、複製に関する禁止事項を示す画面が含まれている。コンテンツを再生するに当たって、これらの事項は、ユーザに必ず知らせておく必要がある。ところが、通常、多くのユーザは、このような事項が示されている画面をスキップしてしまい、著作権や複製に関する禁止事項等の確認が徹底できない。上述のように、平文データ部に、著作権や複製に関する禁止事項の画面を記録しておけば、ユーザがこの画面を見なければコンテンツの映像データを再生できないことになり、著作権や複製に関する禁止事項等をユーザに確認させたり、著作権者がだれであるかを確認させることができる。

【0 1 2 5】また、例えば、映画のビデオデータのコンテンツに、そのコンテンツを提供している企業のコマーシャルが含まれているとする。この場合、通常、多くのユーザは、再生時に、そのコマーシャルの部分をスキップしてしまう。そのコンテンツを提供している企業側になると、コマーシャルの部分をスキップされてしまうと、そのコマーシャルの効果が十分に得られず、コマーシャルのために支払った宣伝広告費が回収できない。上述のように、平文データ部にコマーシャルを記録しておく
10 と、ユーザは、コマーシャルを見なければ、コンテンツの映像データを再生できなきことになり、コマーシャルを確実に見せることができ、コマーシャルの提供の不利益がなくなる。

【0 1 2 6】なお、上述の例では、ユーザに必ず知らせておきたい情報として、コンテンツの製作者を代表するような画面、著作権の保護に関する事項の警告を示す画面、コマーシャルの画面について説明したが、このような情報は他にも種々のものが考えられる。例えば、長時間に分かる映画のコンテンツの場合の休息中の画面や、音楽のコンテンツの場合の曲償還の画面等が考えられ
20 る。また、ゲームデータの場合には、ゲームの最初の製作者を代表するような画面等が考えられる。その他、種々のものが考えられる。

【0 1 2 7】

【発明の効果】この発明によれば、コンテンツのファイルには、コンテンツのデータを暗号化せずに記録する平文データ部と、コンテンツのデータを暗号化して記録する暗号化データ部とが設けられ、平文データ部では、コンテンツのデータが暗号化せずに記録され、暗号化データ部ではコンテンツのデータが暗号化されて記録される。
30 そして、暗号化のための鍵の少なくとも一部が平文データ部におけるコンテンツのデータに付加情報として埋め込まれている。

【0 1 2 8】再生時には、平文データ部のコンテンツのデータに重畳されて記録されているウォータマークに含まれるキー情報を使用して、それに続く暗号化部のデータの復号化処理が行われる。

【0 1 2 9】このため、ウォータマークの情報を検出しないと、暗号化データ部のデータが再生できなくなるため、ウォータマークの情報が必ず再生される。よって、ウォータマークに含まれているコピーや再生を管理するための情報が必ず得られるようになり、ウォータマークによる著作権の管理が確実に行われるようになる。

【0 1 3 0】また、暗号化のための鍵情報を含むウォータマークが埋め込まれる平文データ部に、ユーザに必ず知らせておきたい情報を記録しておく
40 と、ユーザは、この必ず知らせておきたい情報を再生しなければ、暗号化データ部のコンテンツを復号して再生することができなくなる。

50 【0 1 3 1】したがって、平文データ部に、著作権や複

製に関する禁止事項の画面を記録しておけば、ユーザがこの画面を見なければコンテンツの映像データを再生できないことになり、著作権や複製に関する禁止事項等をユーザに確認させることができる。また、平文データ部にコマーシャルを記録しておく、ユーザは、コマーシャルを見なければ、コンテンツの映像データを再生できないことになり、コマーシャルを確実に見せることができ、コマーシャルの提供の不利益がなくなる。

【図面の簡単な説明】

【図 1】この発明の一実施の形態の説明に用いる略線図である。

【図 2】ウォータマークのエンコーダの一例のブロック図である。

【図 3】ウォータマークのデコーダの一例のブロック図である。

【図 4】この発明が適用されたデータ記録装置の一例のブロック図である。

【図 5】データ記録媒体の説明に用いる略線図である。

【図 6】この発明が適用されたデータ再生装置の一例のブロック図である。

【図 7】この発明の一実施の形態の説明に用いる略線図である。

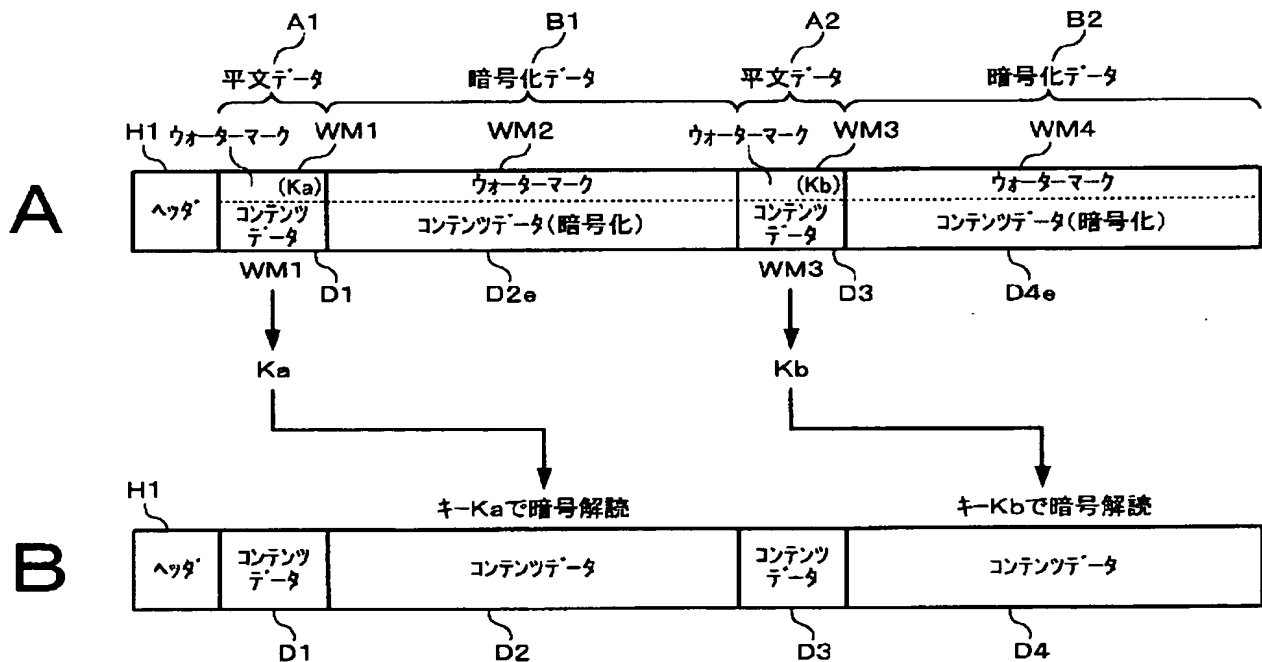
【図 8】この発明の一実施の形態の説明に用いる略線図である。

【図 9】この発明の一実施の形態の説明に用いる略線図である。

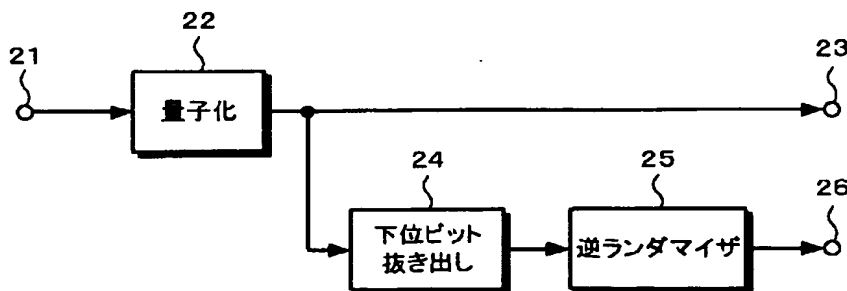
【符号の説明】

A 1、A 2、…平文データ部、B 1、B 2、…暗号化データ部

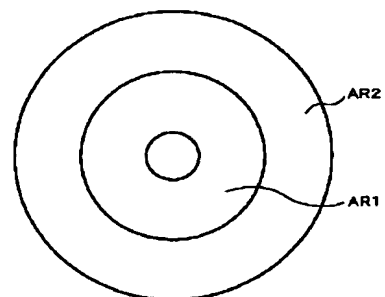
【図 1】



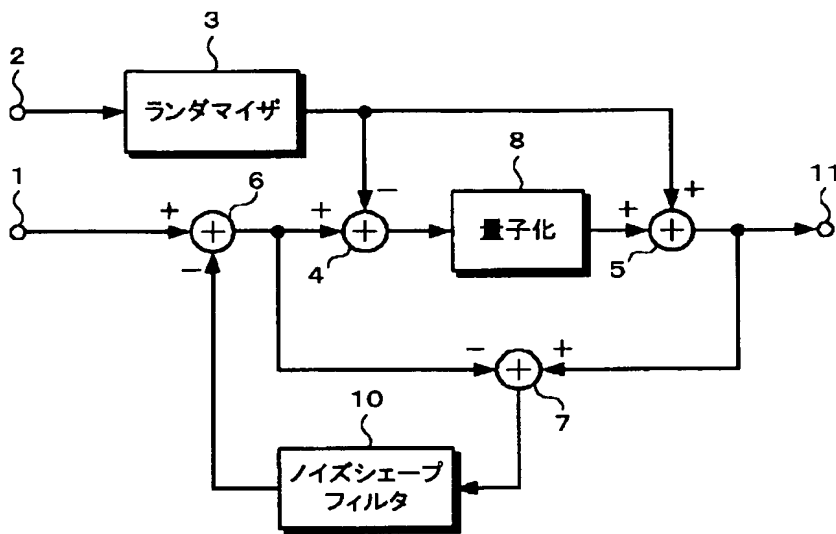
【図 3】



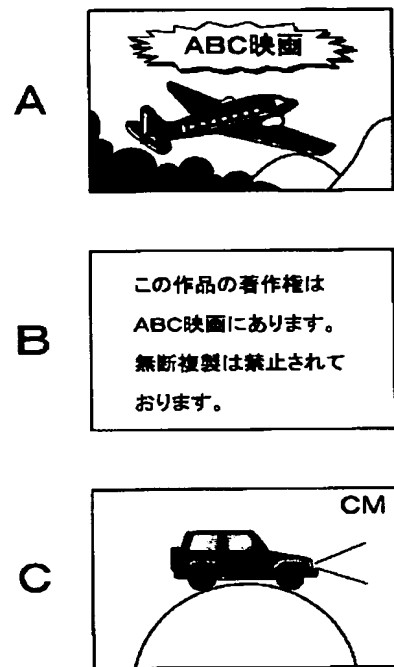
【図 5】



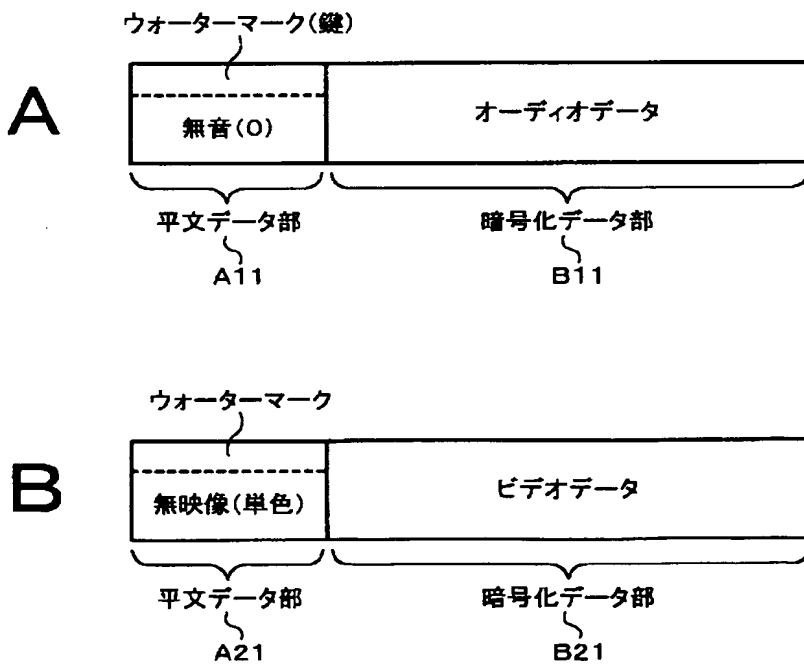
【図 2】



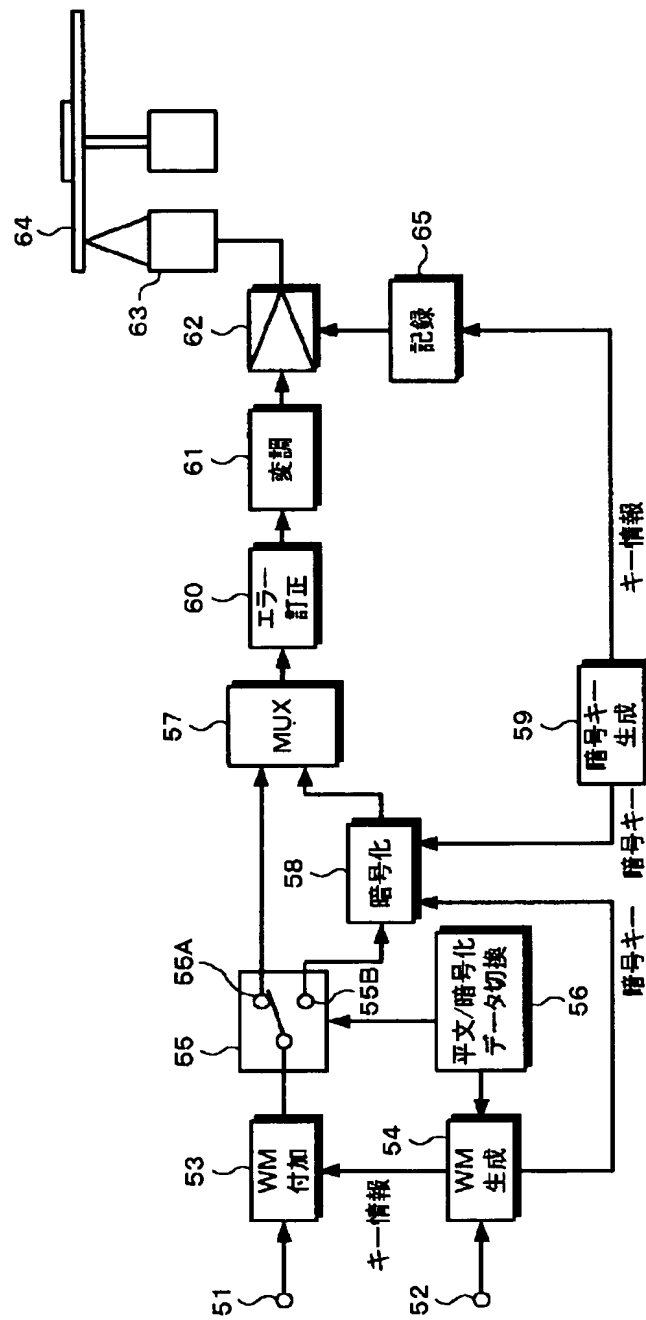
【図 9】



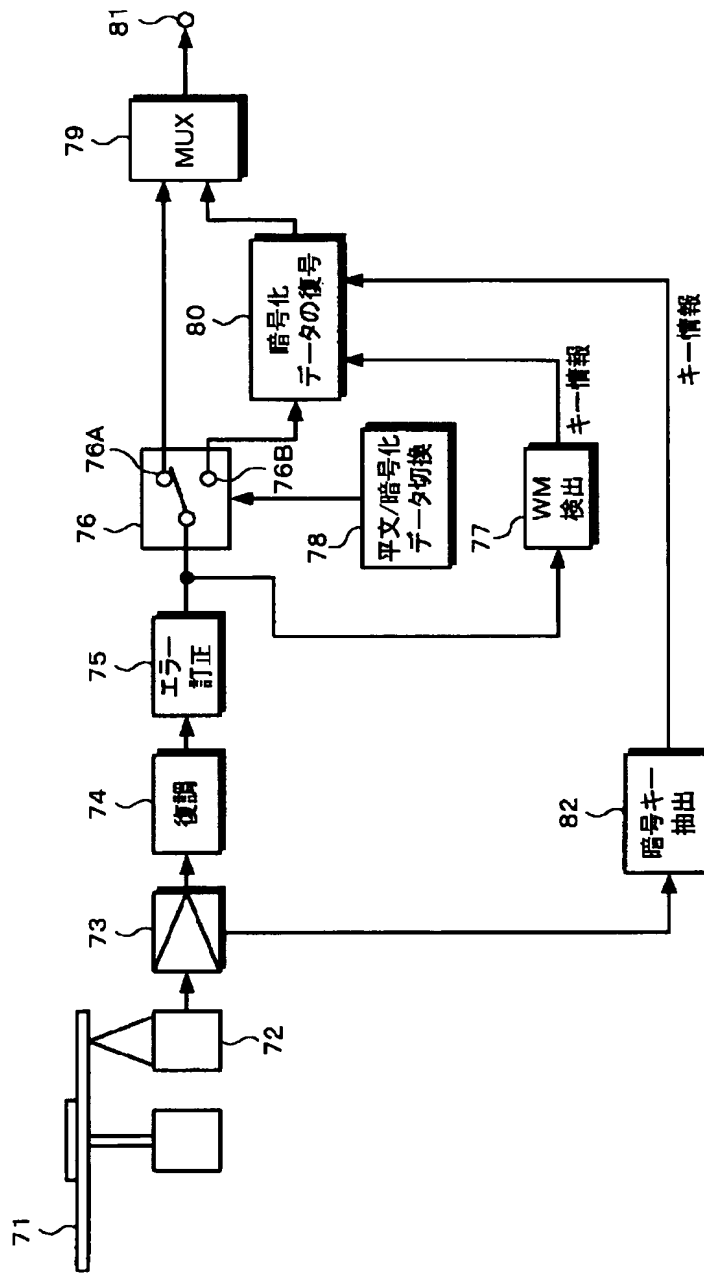
【図 7】



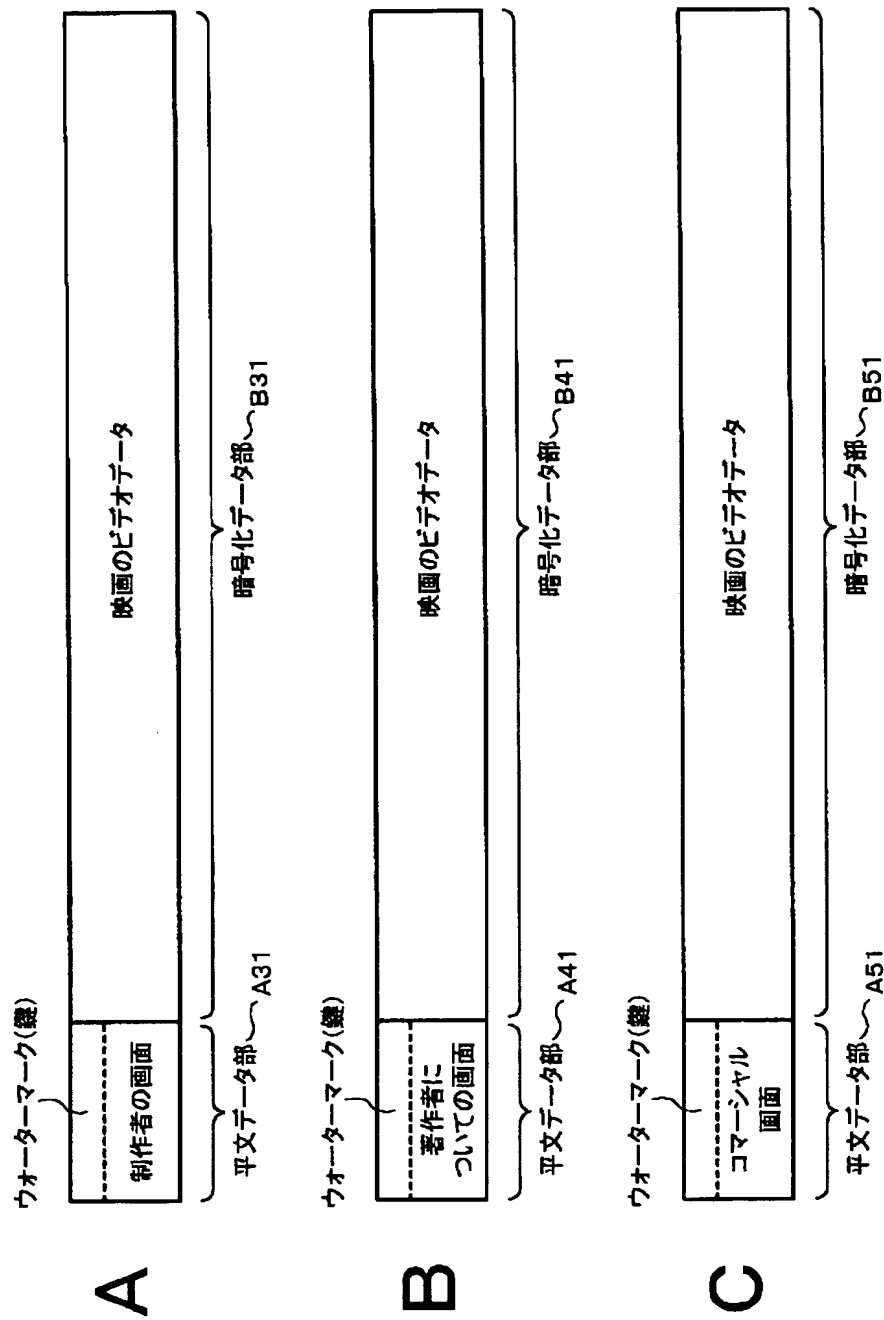
【図 4】



【図 6】



【図 8】



フロントページの続き

(51) Int. Cl. ⁷

G 1 0 L 11/00
H 0 4 L 9/08
H 0 4 N 5/85
5/91

識別記号

F I

G 1 0 L 9/00
H 0 4 L 9/00
H 0 4 N 5/91

テーマコード(参考)

E
6 0 1 B
6 0 1 E
P

F ターム (参考) 5B017 AA06 BA07 CA16
5C052 AA02 AB02 CC12 DD04
5C053 FA13 GB06 GB15 HA40 JA21
KA22
5C063 AB05 AC01 AC05 CA20 CA23
CA31 CA36 DA07
5J104 AA01 AA14 AA16 EA04 EA16
NA02 PA14